

⑫ 公開特許公報(A) 平2-93487

⑬ Int.Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)4月4日

G 09 C 1/00

7368-5B

審査請求 未請求 請求項の数 3 (全4頁)

⑮ 発明の名称 鍵書込み装置

⑯ 特 願 昭63-246735

⑰ 出 願 昭63(1988)9月29日

⑱ 発 明 者 宮 口 庄 司 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

⑲ 発 明 者 栗 原 定 見 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

⑳ 発 明 者 岡 本 龍 明 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

㉑ 出 願 人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号

㉒ 代 理 人 弁理士 草 野 卓

明 細 書

1. 発明の名称

鍵書込み装置

2. 特許請求の範囲

(1) 端末コードの X_i を入力し、秘密パラメータ P を用い、但し P は単一の場合と複数の場合があり、鍵生成手段により、 $K_i = F(P, X_i)$ は鍵生成手段機能の関数表現、として鍵 K_i を決める、ここで関数 F は、乱数生成アルゴリズム、又は暗号アルゴリズム、又はデータ圧縮アルゴリズム、又は法 n のモジュロ演算のいずれかである、以上により鍵 K_i を決める特徴を有する鍵書込み装置。

(2) 前記鍵生成手段は、 $K_i = F(PG_i, X_i)$ として鍵 K_i を決め、ここで、 $PG_i = f_1(P, G_i)$ 、 f_1 は P と G_i の関数、 P は前記秘密パラメータ、 G_i は保護コード、である特徴を有する請求項1の鍵書込み装置。

(3) 前記鍵生成手段は、 $K_{iu} = F(P, Q_{iu})$ として n 個の鍵 K_{iu} を決め($u = 1, 2, \dots, n$)、ここで、 $Q_{iu} = f_2(X_i, X_{iu})$ 、 f_2 は X_i と X_{iu} の

関数、 P は前記秘密パラメータ、 X_{iu} は副端末コード、である特徴を有する請求項1の鍵書込み装置。

3. 発明の詳細な説明

「産業上の利用分野」

この発明は、暗号の鍵、メッセージの改ざん検出のためのメッセージ認証の鍵、通信相手を確認する相手認証の鍵、或はデジタル署名等を使う秘密情報を生成する装置に関するものである。

「従来の技術」

個々の端末をネットワーク内で識別するための端末コードを、記号 X_i で表す($i = 1, 2, \dots$)。端末コードは、例えば利用者の電話番号や利用者識別番号であり、公開できる情報である。端末コード X_i を元に、利用者個別の秘密の鍵 K_i を生成するには、従来は、例えば適当な関数 F' を用い、 $K_i = F'(X_i)$ により生成していた。従来の鍵書込み装置は、関数 F' が一旦第三者に知られると、端末コードから鍵 K_i が簡単に算出出来、鍵 K_i の秘密を保てないという欠点がある。

「課題を解決するための手段」

秘密パラメータPを用いて鍵Kiを生成する。即ち、 $Ki = F(P, Xi)$ 、Fは鍵生成手段の機能の関数表現、により鍵Kiを算出する。ここでパラメータPは、端末側に秘密にすることが特徴である。Fが外部に知られてもパラメータPを変えることによりKiの秘密を保てる。鍵書き込み装置はその内部に、秘密パラメータPの書き込みは可能であるが、「Pの読み出しは不可能なP保持手段」を設ける。一人の安全責任者が、多数の鍵書き込み装置に同じ秘密のパラメータPを投入し、鍵書き込み装置内部のP保持手段にパラメータPを保持する。P保持手段は、例えばLSI（大規模集積回路）内部のメモリに電池により保持（バッテリーバックアップ）することにより、あるいは、金属製の丈夫な箱を作り、これにROMを入れ物理的な錠を備えることにより実現する。鍵書き込み装置に端末コードのXiを入力すると、鍵生成手段により、鍵Kiを生成する。この鍵書き込み装置から秘密のパラメータPを取り出すことはできない。

データ圧縮アルゴリズムとして、ディジタル署名の分野で使われるハッシュ関数を用いても良い。

第四の方法は、法nのモジュロ演算により関数Fを実現する。モジュロ演算は例えば、 $F(y1, y2) = F(P, Xi) = (Xi)^y \mod n$ 、ここでパラメータPは2つのパラメータ $P = (d, n)$ とからなり、 $\mod n$ は、法nのモジュロ演算である。

次に $F(y1, y2)$ のy1とy2について説明する。y1は、Giを用いないときは $y1 = P$ であり、Giを用いるときは、例えば $y1 = f1(P, Gi) = P \oplus Gi$ あるいは、 $y1 = f1(P, Gi) = P \oplus Gi$ とする。ここで、 $a \oplus b$ は、データaとbを並べて出来るデータを表す。 $a \otimes b$ は、aとbの排他的論理和を表す。y2は、Xiuを用いないとき $y2 = Xi$ であり、Xiuを用いるときは、例えば $y2 = f2(Xi, Xiu) = Xi \oplus Xiu$ 、あるいは、 $y2 = f2(Xi, Xiu) = Xi \otimes Xiu$ とする。Giは保護コードと呼ばれるものであり後述する。

「実施例1」

第1図はこの発明に基づく、鍵書き込み装置1の

「Fの実現方法」

第一の方法は、乱数生成アルゴリズムにより関数Fを実現する。即ち、 $F(y1, y2) = R(y1, y2)$ 、 $R(y1, y2)$ は乱数生成アルゴリズムであり、y1は関数Rの第1の初期値であり、y2は関数Rの第2の初期値である。 $R(y1, y2)$ は、y1とy2が与えられたとき、乱数値 $R(y1, y2)$ の値が確定する性質を有する乱数生成アルゴリズムである。

第二の方法は、暗号アルゴリズムにより関数Fを実現する。即ち、 $F(y1, y2) = E(y1, y2)$ ここで、 $E(y1, y2)$ は暗号アルゴリズムであり、y1は暗号化の鍵、y2は入力データとし、暗号文 $C = E(y1, y2)$ を出力する。

第三の方法は、データ圧縮アルゴリズムにより関数Fを実現する。即ち、 $F(y1, y2) = H(y1, y2)$ 、ここで、 $H(y1, y2)$ はデータ圧縮アルゴリズムであり、y1は初期値、y2は入力データ、であり初期値y1の条件で入力データy2をデータ圧縮し圧縮結果の $H(y1, y2)$ を出力する。

一実施例のブロック図であり、鍵生成手段2、P保持手段3、物理保護手段4、鍵書き込み手段5、P入力部6、ID入力部7からなる。鍵生成手段2は、パラメータPをP保持手段3から入力し、端末コードのXiをID入力部7から入力し、鍵Kiを生成し、この結果を鍵書き込み手段5へ伝える。P保持手段3は、例えば、パラメータPを一時メモリに記憶する。物理保護手段4はパラメータPを鍵書き込み装置の外部から変更できるが、Pを外部に読み出せない性質、又は読みだそうとするとPの値を破壊する性質を持たせる。例えば、物理保護手段4は、読出し端子が外部に露出されていないLSIとして実現し、あるいは、金属製の箱を作りこれにROMを入れ物理的な錠を付加することにより実現する。書き込み手段5は、例えばROM書き込み器であり、鍵生成手段2で生成した鍵Kiを、ROMに書き込む。他の書き込み手段5の実施例は、ICカード書き込み器であり、この場合は、生成された鍵Kiを、ICカードに書き込む。

この鍵書込み装置を動作させるには、まず、P入力部6から秘密のパラメータPを入力し、PをP保持手段3に保持する。鍵生成手段2は端末コードのXiをID入力部7から入力し、P保持手段内に保持しているパラメータPを用い、 $Ki = F(P, Xi)$ により鍵Kiを決め、得られたKiを鍵書込み手段5へ伝え、鍵書込み手段5は鍵Kiを、例えばICカードに書き込む。

なおP保持手段3を省いてもよく、この場合はこの鍵書込み装置を使う都度、パラメータPを鍵生成手段2に入力する。

「実施例2」

実施例1において、パラメータPはdとnからなり、即ち $P = (d, n)$ であり、P入力部6はdとnを入力し、P保持手段3はdとnを保持し、鍵生成手段2は、次の演算を行う。

$$Ki = F((d, n), Xi) = (Xi)^d \bmod n$$

但し、 $\bmod n$ は、法nのモジュロ演算を表す。

この鍵書込み装置を動作させるには、まず、P入力部6から秘密のパラメータのdとnを入力し、

を決め、ここで $f1(P, Gi)$ はPとGiの関数であり、たとえば $f1(P, Gi) = P \parallel Gi$ や、 $f1(P, Gi) = P \oplus Gi$ である（ \parallel はデータの連結、 \oplus は排他的論理和）。

以上により鍵Kiと保護コードGiを鍵書込み手段に書き込む。

なおP保持手段3を省いてもよく、この場合はこの鍵書込み装置を使う都度、パラメータPを鍵生成手段2に入力する。

「実施例4」

実施例1において、入力部は端末コードのXiと共に副端末コードのXiu（ $u = 1, 2, \dots$ ）をも入力する機能を含む。

この鍵書込み装置を動作させるには、まず、P入力部6から秘密のパラメータPを入力し、PをP保持手段3に保持する。端末コードのXiと共に副端末コードのXiuをID入力部7から入力し、P保持手段中の秘密パラメータPを用い、 $Ki = F(P, Xi \oplus Xiu)$ 、但し、 $u = 1, 2, \dots$ 、により鍵Kiuを算出する。

dとnとをP保持手段3に保持する。端末コードのXiをID入力部7から入力し、P保持手段中のパラメータ $P = (d, n)$ を用い、 $Ki = (Xi)^d \bmod n$ により秘密の情報Kiを決め、鍵書込み手段5へ出力する。

なおP保持手段3を省いてもよく、この場合はこの鍵書込み装置を使う都度、パラメータPを鍵生成手段2に入力する。

「実施例3」

実施例1において、鍵生成手段2は乱数生成機能をも含み、ここで生成した乱数を保護コードGiと決め、鍵Kiと保護コードGiを鍵書込み手段に出力する機能を有する。

この鍵書込み装置を動作させるには、まず、P入力部6から秘密のパラメータPを入力し、PをP保持手段3に保持する。端末コードのXiをID入力部7から入力し、P保持手段中の秘密パラメータPを用い、端末コードXiを入力し、乱数生成などにより保護コードGiを生成し、 $Ki = F(PGi, Xi)$ 、但し $PGi = f1(P, Gi)$ 、により鍵Ki

なおP保持手段3を省いてもよく、この場合はこの鍵書込み装置を使う都度、パラメータPを鍵生成手段2に入力する。

「Kiの使い方の例」

Kiの使い方の例を説明する。

センタと複数のICカード入出力装置を通信回線で接続したシステムを考える。ICカード保持者は、適当なICカード入出力装置と通信回線を介して、センタと情報を交換する。センタと各ICカード間で例えばメッセージ認証用に、鍵Kiを使う。各ICカードは、この発明の鍵書込み装置により、それぞれ個別の鍵Kiを内部に保持している。センタは、各ICカードに端末コードのXiを問い合わせて入手し、鍵Kiを算出して生成する（センタは、鍵生成手段とパラメータPを持つ）。

このようなICカード利用システムでは、ICカードの発行数が膨大となることが考えられる。大規模なICカード利用システムを運用するには、鍵Kiが外部に漏れないように安全な方法でICカード別の鍵を生成する業務が必要であり、鍵生

成方法が第3者に漏れないこの発明による鍵書込み装置が有効である。

Kiの使い方の他の例を説明する。センタと複数の端末を通信回線で接続したシステムを考える。センタと各端末間で例えばメッセージ認証用に、鍵Kiを使う。各端末はこの発明の鍵書込み装置により、それぞれ個別の鍵Kiと保護コードGiを内部に保持している。センタは、各端末に端末コードのXiと保護コードを問い合わせて入手し、鍵Kiを算出して生成する。端末コードは、端末に付与した電話番号を使う。端末を売買するなどにより電話番号Xiが変わらずに端末所有者が変わった場合、センタは端末の保護コードGiを変更する。すると鍵Kiが変わる。古い鍵Kiが使えなくなるので、端末の旧所有者が新しい鍵Kiを知ることは出来ず安全である。

デジタル署名等において、Kiを秘密情報として使う方法については、例えば次の文献、「黒沢肇著、鍵変更の容易なID暗号方式、電子情報通信学会技術研究報告(Vol. 88, No 33)、情報

セキュリティ、論文番号 ISEC 88-6」に解説されている。

「発明の効果」

この発明による鍵書込み装置は、パラメータPを書き込むことは可能であるが、逆の操作、即ち、パラメータPを鍵書込み装置から読み出すことは出来ない。このため、端末コードXiを知られても、パラメータPが秘密であるので、鍵Kiを生成出来ない。この発明の鍵書込み装置を使うことにより、鍵Kiの生成規則を秘密に保つことが容易であり、安全性を確保出来る。

4. 図面の簡単な説明

第1図は、この発明に基づく鍵書込み装置の実施例のブロック図である。

特許出願人 日本電信電話株式会社
代理人 章 野 卓

図 1

